Patent
Attorney's Docket No. 032559-077

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Johan SÖDERBERG et al.	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: March 9, 2001	)	
	)	
For: Improved Bit Error Resilience for an Internet Protocol Stack	)	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Before examination of this application, please enter the following amendment.

IN THE SPECIFICATION

Page 1, line 3, replace the heading with --BACKGROUND--; and
line 10, delete in its entirety.

Page 7, line 18, replace the heading with --SUMMARY--.

Page 12, line 1, replace the heading with --DETAILED DESCRIPTION--.

IN THE CLAIMS

9. (Amended) The bit error resilience method according to claim 7, wherein said packets include compressed real-time data and said higher-level error protection of at least part of the payload includes the step of protecting critical real-time parameters in the payload.

10. (Amended) The bit error resilience method according to claim 5, wherein said step of protecting header information in said header compressed packets includes the step of protecting at least part of the compressed header by a local checksum, wherein the local checksum is selected as a local subset of said compressed header.

16. (Amended) The bit error resilience method according to claim 10, wherein said header compressed packets are header compressed according to one of the following standards:

RFC 2507 of the Internet Engineering Task Force (IETF);

RFC 2508 of the IETF; and

Robust checksum-based header compression (ROCCO) of the IETF.

28. (Amended) The method according to claim 22, wherein said header compressed packets are header compressed according to one of the following standards:

RFC 2507 of the Internet Engineering Task Force (IETF);

RFC 2508 of the IETF; and

Robust checksum-based header compression (ROCCO) of the IETF.

37. (Amended) The bit error resilience system according to claim 35, wherein said packets include compressed real-time data and said higher-level error protection of at least part of the payload is effectuated by means for protecting critical real-time parameters in the payload.

38. (Amended) The bit error resilience system according to claim 33, wherein said means for protecting header information in said header compressed packets includes means for protecting at least part of the compressed header by a local checksum, wherein the local checksum is selected as a local subset of said compressed header.

44. (Amended) The bit error resilience system according to claim 38, wherein said header compressed packets are header compressed according to one of the following standards:

RFC 2507 of the Internet Engineering Task Force (IETF);

RFC 2508 of the IETF; and

Robust checksum-based header compression (ROCCO) of the IETF.

57. (Amended) The system according to claim 50, wherein said header compressed packets are header compressed according to one of the following standards:

RFC 2507 of the Internet Engineering Task Force (IETF);

RFC 2508 of the IETF; and

Robust checksum-based header compression (ROCCO) of the IETF.

IN THE ABSTRACT

Please replace the Abstract, found on page 31, with the new Abstract attached as a separate sheet.

REMARKS

The specification, claims, and Abstract have been amended to place the application in better form for examination. Favorable consideration is respectfully solicited.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Theodosios Thomas

By: Reg 45,159

for Michael G. Savage
Registration No. 32,596

P.O. Box 1404
Alexandria, Virginia 22313-1404
1 919 941 9240

Dated: March 9, 2001

"Express Mail" mailing label No EL 766106006US
Date of Deposit: March 9, 2001
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner of Patents, Washington DC 20231

Judith Harris

March 9, 2001
Date

ABSTRACT

The invention concerns the bit error resilience of an IP protocol stack based on a secure link layer, in which packet flows are header compressed according to a suitable header compression standard. By analyzing each packet at the link layer, it can be determined whether the packet is a full header packet, in which case the link layer checksum evaluation is used as normal for discarding faulty full header packets, or a header compressed packet, in which case the link layer checksum evaluation is ignored and the packet is propagated upwards in the protocol stack. This solution not only allows for more intelligent higher-level handling of faulty header compressed packets, but also solves the problem of properly protecting full header packets at the link layer. In order to compensate for ignoring the link layer checksum evaluation for header compressed packets, header protection is introduced at the header compression level of the link layer by using one or more local checksums. The invention is particularly applicable to delay-sensitive real-time data such as compressed voice or video.

Attachment to Preliminary Amendment dated March 9, 2001

Marked-up Copy of Changes to the Specification

Page 1, heading at line 3

[TECHNICAL FIELD OF THE INVENTION] BACKGROUND

Page 1, heading at line 10

[BACKGROUND]

Page 7, heading at line 18

SUMMARY [OF THE INVENTION]

Page 12, heading at line 1

DETAILED DESCRIPTION [OF EMBODIMENTS OF THE INVENTION]

Attachment to Preliminary Amendment dated March 9, 2001

Marked-up Copy of Amendments to the Claims

9. (Amended) The bit error resilience method according to claim 7 [or 8], wherein said packets include compressed real-time data [such as compressed voice or video,] and said higher-level error protection of at least part of the payload includes the step of protecting critical real-time parameters in the payload.

10. (Amended) The bit error resilience method according to claim 5, wherein said step of protecting header information in said header compressed packets includes the step of protecting at least part of the compressed header by a local checksum, [which] wherein the local checksum is selected as a local subset of said compressed header.

16. (Amended) The bit error resilience method according to claim 10 [or 11], wherein said header compressed packets are header compressed according to one of the following standards:

RFC 2507 of the Internet Engineering Task Force (IETF);

RFC 2508 of the IETF; and

Robust checksum-based header compression (ROCCO) of the IETF.

28. (Amended) The method according to claim 22 [or 23], wherein said header compressed packets are header compressed according to one of the following standards:

RFC 2507 of the Internet Engineering Task Force (IETF);

RFC 2508 of the IETF; and

Robust checksum-based header compression (ROCCO) of the IETF.

37. (Amended) The bit error resilience system according to claim 35 [or 36], wherein said packets include compressed real-time data [such as compressed voice or video,] and said higher-level error protection of at least part of the payload is effectuated by means for protecting critical real-time parameters in the payload.

38. (Amended) The bit error resilience system according to claim 33, wherein said means for protecting header information in said header compressed packets includes means for protecting at least part of the compressed header by a local checksum, [which] wherein the local checksum is selected as a local subset of said compressed header.

44. (Amended) The bit error resilience system according to claim 38 [or 39], wherein said header compressed packets are header compressed according to one of the following standards:

RFC 2507 of the Internet Engineering Task Force (IETF);

RFC 2508 of the IETF; and

Robust checksum-based header compression (ROCCO) of the IETF.

57. (Amended) The system according to claim 50 [or 51], wherein said header compressed packets are header compressed according to one of the following standards:

RFC 2507 of the Internet Engineering Task Force (IETF);

RFC 2508 of the IETF; and

Robust checksum-based header compression (ROCCO) of the IETF.